Kentucky Governor's Office for Technology

Security Awareness Newsletter

Published by the GOT Division of Security Services

January 2004 **Volume 11, Issue 1**

Inside this issue:

Enterprise Computer Sanitization Policy

Have you ever bought something second-hand and found it contained personal information from the original owner such as receipts, notes, or correspondence? This same situation could also occur with surplus computer equipment possibly resulting in the accidental divulgence of sensitive and/or confidential data.

In fact, there are many stories of sensitive information such as credit card numbers, medical information, and emails that have been found on used computers. Even if the data on the computer has been deleted or the hard drive formatted, the new owner can use various software available on the market today to recover the data.

To ensure that this scenario does not happen to State computer equipment, the Commonwealth developed the Sanitization of IT Equipment and Electronic Media Policy (CIO-077), which requires all computers and other electronic media slated for surplus, transfer, or disposal to be adequately purged of all sensitive/confidential data.

Since standard formatting alone is not enough to permanently delete data and prevent its recovery, the enterprise computer sanitization policy provides detailed procedures for using the correct sanitization methods to effectively remove sensitive/confidential data from computers, as well as other electronic media and components. Some of the most common methods for properly sanitizing hard drives include:

—Physically destroying the hard drive, making it unusable.
—Degaussing the drive using electromagnetic energy to erase all data. *(Please note that this method may also make the drive unusable.)*
—Overwriting the hard drive using special clearing and sanitization software to prevent the data from being recovered. (*This method will not harm the hard drive and is recommended for PCs that will be reused.)*

The Commonwealth's policy follows stringent US Department of Defense (DoD) sanitization standards and provides detailed overwriting, physical destruction, and degaussing specifications. The Commonwealth recommends the following software products: WipeDrive for disks and SecureClean for files. These software conform to DoD guidelines and are on the Commonwealth's approved products list. So when you are ready to get rid of that old PC, make sure the PC is the only thing you give away.

What Really Happens When We Delete—When we delete a file such as a Word or Excel document, Windows does not actually delete it. It only deletes its reference to the name and location on the hard drive. The actual file remains on the hard drive until it is overwritten by other files. Any data recovery software can recover a deleted file if it has not been overwritten, and more advanced software can even retrieve the overwritten files. Standard formatting of a hard drive using *Format* or *F-Disk* will not permanently delete data either. The only sure way to make data unrecoverable is to either destroy the hard drive or to use special clearing software that adheres to the US DoD computer sanitization standard that requires overwriting the hard drive three times with random characters.

GOT's Response to Homeland Security

After September 11, 2001, the country began focusing on ways to prevent tragedies such as the destruction of the World Trade Centers in New York City from reoccurring. The federal government took the lead by establishing the Office of Homeland Security (later renamed the U.S. Department of Homeland Security). One of the tasks undertaken by the Office of Homeland Security was to devise a Homeland Security Advisory System that would inform citizens of current terrorist threat conditions and provide suggested protective measures.

GOT has followed suit by developing its own Homeland Advisory Security Alert Plan to protect its employees and infrastructure. The Plan outlines potential steps to be implemented by various GOT organizations for each security alert level. As the national threat level is elevated, GOT executive management meets to determine appropriate steps to implement as outlined by the particular threat level in the Plan.

In order to adequately secure the Commonwealth Data Center (CDC), GOT began renovation in June 2003 to increase security at the facility.

In addition, GOT strives to keep its employees informed of the latest homeland security initiatives by publishing articles in its bi-monthly security awareness newsletter, as well as conducting homeland security awareness sessions. GOT also maintains an electronic homeland security library available to all GOT staff on GOTSource.

On December 20, 2003, the national homeland security threat level was once again elevated to Orange (indicating a high threat of a terrorist attack). In response, GOT activated level Orange procedures from its Homeland Advisory Alert Plan, which include enhanced security precautions such as increased monitoring by security staff and the restriction of visitors and non-essential personnel to the Commonwealth Data Center (CDC) for the duration of the alert (see the GOT Homeland Advisory Security Alert Plan for more information).

Since the Homeland Security Advisory System was introduced in March 2002, GOT has activated level Orange procedures on five occasions, following the nation's lead.

If you would like more information on Homeland Security, please refer to the following websites:

homeland.kentucky.gov — Kentucky's homeland security website designed to provide current information on homeland security issues in the Commonwealth.

www.cdc.gov — Federal Centers for Disease Control and Prevention. Provides information on bioterrorism and other public health related matters. Click on "Terrorism and Public Health" to left.

www.dhs.gov/dhspublic — U.S. Department of Homeland Security home page. Provides a vast resource of information on threats and protection, latest homeland security news, planning and preparedness for emergencies and disasters, etc.

www.ready.gov — Site developed by the U.S. Department of Homeland Security to provide a readiness checklist for citizens.

www.cdc.gov/niosh/topics/prepared — National Institute of Occupational Safety and Health's emergency preparedness guidelines.

www.redcross.org/services/disaster/keepsafe/unexpected.html — Red Cross disaster planning page.

Did you know . . .
The number of employees working for the federal Department of Homeland Security—170,000
The number of government agencies that merged under the department—22
Homeland Security's 2003 IT budget—$2.13 billion
Source: Input

Security Issues with Handheld Devices

The use of handheld devices such as personal digital assistants (PDAs) is rapidly growing due to their convenience and relatively inexpensive cost when compared to laptops. The storage capacity of these devices has also increased, easily providing enough space to download an organization's data for work at home or while traveling. Unfortunately, the security issues with handheld devices are the same for most other computer equipment. Some of the issues include:

—Theft or loss of the device. According to IT research and advisory firm, Gartner, over 250,000 cell phones & PDAs will be lost at airports.
—Users not enabling the password feature.
—Hackers with physical possession of the devices can import password protected files to a file viewer.
—Malicious code is becoming an increasing problem. If devices become infected, they can transfer viruses to the network.
—Unauthorized network access. Device users often use the same password for their PDA as they do for the network. There are many hacker tools available to steal a PDA's password list and certificate files, possibly exposing the network.
—Susceptibility to "eavesdropping" due to handheld's wireless transmission capability.
—Reports of wireless network crashes due to the extra traffic.
—Device retrieval. Retrieving the devices after dismissal, job transfer, etc.

Because handheld devices extend an organization's network, all points of access need to be secured including access from these devices. At this time, the industry is developing security measures such as built-in firewalls on chips and file encryption available via add-on programs. Also, since the devices are so small, the risk of them being lost or stolen is substantial. This fact alone is enough to raise a red flag for security personnel, especially if sensitive/confidential data is downloaded onto one of these devices or if hackers use them to gain access to the network. The bottom line is that organizations need to be aware of these issues and develop the necessary policies and procedures for handheld device usage while educating their users of the potential security risks. Information on the Commonwealth's Wireless LAN Enterprise Policy can be found by clicking here.

Disabling Unneeded Network Services

The following article is intended for network administrators. —Any service or application running on a network is a potential source for attack. By default, many operating systems install auxiliary services that are not needed such as FTP server, telnet, and a web server. Industry best practices recommend that any unneeded service be disabled or removed. The rule of thumb should be, if you are unsure of what the service is, disable it.

By disabling unneeded services, you also increase the performance of systems by reducing the amount of resources needed such as memory and CPU cycles. For those services that are needed, especially those on computers that host public services such as HTTP, FTP, mail & DNS services, security patches should be kept up-to-date to prevent possible exploit by intruders. For more information on Windows services, check out the Winnetmag.com article entitled Dangerous Services by Randy Franklin Smith.

Did you know . . .
According to the Eighth Annual 2003 CSI/FBI Computer Crime and Security Survey:
— Theft of propriety information caused the greatest financial loss in 2003.
— The second most expensive computer crime among survey respondents was denial of service.
— Seventy-five percent (75%) of survey respondents acknowledged financial losses due to computer security breaches.

Social Engineers: What to Watch Out For

Unfortunately, the term 'social engineer' that we are referring to is not a fancy word for a professional party planner. Long before the information age, a term such as con artist may have been used, but whichever name you prefer, these culprits can be tenacious and dangerous in their pursuit of an individual's or organization's sensitive information. Social engineers are manipulators who take advantage of our natural tendency to trust. They usually acquire information by contacting multiple employees within an organization, compiling names and other information before they strike, either physically or remotely via computer to gain access to sensitive information. Their motives may be simply for sport or for more heinous purposes such as committing fraud, industrial espionage, or personal identify theft with the information obtained. A list of common methods of attack are listed below to help educate employees to the type of tactics that social engineers often employ:

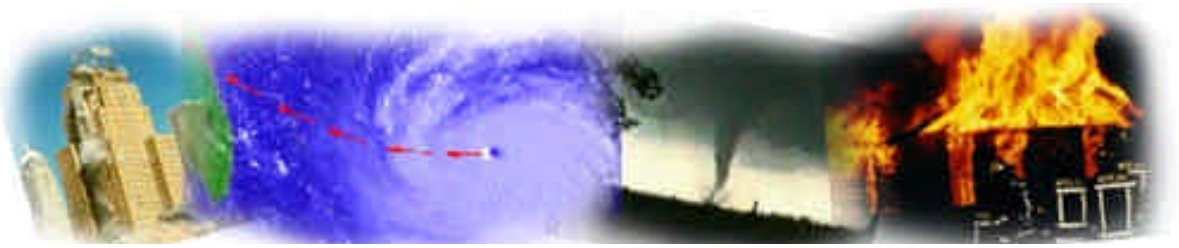
Phone Attack—The social engineer usually impersonates someone in authority to get information from a user. Help Desks are usually a prime target for this type of attack since the nature of their business is to help people. Another example would be someone calling in the middle of the night claiming to be from the telephone company informing you that long distance calls have been made from your number and that you will have to pay the bill unless you give them your calling card number and pin to remove the charges. Another method social engineers often use is shoulder surfing. Whenever you are using your ATM card or calling card in a public place such as hotel or airport, be aware of people that may be watching your every move and recording the selections you make at the money machine or telephone booth. This type of attack can and does happen.

Online Attacks—Social engineers often use the Internet to dupe unsuspecting individuals to provide sensitive information such as passwords, social security numbers, and credit card account numbers. Many of these scams have received publicity in the news such as the Paypal scam that was received as an email requesting users to re-enter their credit card information or other account information because it had been lost during a system crash. Another scheme involves someone posing as the system administrator, sending emails to users requesting their network passwords. Pop-up windows are also often used to request users to enter their userIDs and passwords to fix a problem. Users should be aware of these ploys and never provide their passwords to anyone let alone send them unencrypted over the Internet.

Dumpster Diving—An organization's trash can offer a wealth of information to social engineers. The LAN Times listed the following items as potential security leaks: "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks & tapes, company letterhead and memo forms, and outdated hardware" (see the computer sanitization article on page 1). Any sensitive/confidential information should be shredded or burned before disposal. In fact, GOT policy requires that shredders be placed next to all area printers to allow the safe disposal of sensitive information.

Friendly Persuasion—Social engineers are often successful because the majority of people are trusting and want to help others. One tactic often used in persuading unsuspecting victims is impersonation such as impersonating a computer support person, a manager, a vendor, etc. This is especially useful in a large organization where it is not realistic to know everyone. Conformity is another tactic where the social engineer tries to convince the victim that everyone else has been providing him/her with the information so why don't they do so also.

If you encounter an individual that you believe is trying to acquire sensitive or confidential information from you, report it to your supervisor immediately and submit a Security Incident Reporting Form (GOT-F012) to the GOT Division of Security Services. Also remember that questions regarding state personnel or systems should be forwarded to a supervisor or your agency's Personnel Officer.



Disaster Recovery Awareness

Creating and Implementing a Disaster Recovery Plan

The November 2003 issue of the GOT Security Awareness Newsletter emphasized the importance of having a disaster recovery plan (DRP) in place. This month's issue will focus on the activities necessary to develop and implement an effective disaster recovery plan.

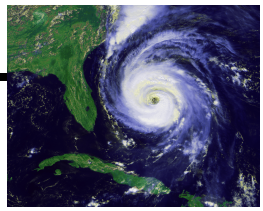
The first step in writing a disaster recovery plan is to get into a mindset of imagining the worst. Think about what possible disasters could occur and the actions needed to restore services to your agency's systems if they were compromised or irretrievably damaged. The steps listed below are a summary of the major tasks needed to develop and implement an effective disaster recovery plan.

Step 1—Conduct a Risk Analysis to identify all risks that could jeopardize system availability or data integrity, including virus threats, human error, or natural disasters such as a fire. In addition, the Risk Analysis should also prioritize the criticality of an agency's applications and systems being sure to include timeframes in which they should be restored. Generally, the shorter the timeframe needed to recover, the greater the cost. Just indicating that an application is needed in 24 hours is not enough. Organizations need to accurately identify a system's criticality in order to determine the monies needed to devote to recovery efforts.

Step 2—Develop a budget. It is always a good idea to include disaster recovery in all budget exercises when possible. Although with the current budget crisis that may be difficult, consider the cost of permanently losing the resources and data needed to run your organization and/or provide services to the public.

Step 3—Create the plan. Copies of the disaster recovery plan should be kept both on and off-site. The plan should include the following:
—What events constitute a disaster.
—What people in the organization have the authority to declare a disaster and can put the plan into effect.
—The roles and responsibilities of all key personnel in respect to carrying out the plan.
—Contact details for all critical IT staff members.
—An inventory of the necessary hardware & software required to restore systems.
—A schedule listing the staff that will be manning the backup site.
—Events necessary to move operations from the backup site to the restored/new data center.
—Specific, detailed steps to accomplish the equipment and application recovery in case key people are unavailable.

Step 4—Test the plan at least annually to ensure employees are well trained in performing their duties in the event of a disaster. Also, record the detailed results of the testing, updating the plan to address any issues that were identified. As an organization's environment changes so should the disaster recovery plan.



Disaster Statistics . . . The ten most expensive natural disasters as ranked by FEMA relief costs:

1. 1994 Northridge, CA earthquake—$7 billion
2. 1998 Hurricane Georges—$2.2 billion
3. 1992 Hurricane Andrew—$1.8 billion
4. 1989 Hurricane Hugo—$1.3 billion
5. 1993 Midwest Floods—$1.1 billion
6. 2001 Tropical Storm Allison—$1.1 billion
7. 1999 Hurricane Floyd—$1 billion
8. 1989 Loma Prieta, CA earthquake—$866 million
9. 1997 Red River Valley Floods—$740 million
10. 1996 Hurricane Fran—$622 million

CYBER BYTES

Current Security News & Information

Microsoft Targets Spammers

Microsoft has taken a firm stance in its recently announced battle against Spam. Since many of the viruses that targeted Microsoft's software products in 2003 were specifically associated with spam, Microsoft is now taking legal action against spammers. For more information, click here.

The Year in Malicious Code

Want to find out what the major virus threats were in 2003 and what the experts predict will haunt us this new year? Check out Help Net Security's article by Berislav Kucan, "A Look into the Viruses that Caused Havoc in 2003."

The CAN SPAM Act

The CAN SPAM (Controlling the Assault of Non-Solicited Pornography and Market) Act was signed into law in late December 2003 by President George W. Bush. CAN SPAM basically established rules and penalties for the Federal Trade Commission to curb unsolicited commercial email (aka Spam). Many anti-Spam organizations are critical of the legislation calling it the "You Can Spam" Act, stating that it legalizes Spam instead of prohibiting it. The good news is that the Act makes it illegal for spammers to use open proxies and false headers, a ploy often used to bypass spam blocks and/or avoid being identified. The Act will also allow ISPs (Internet Service Providers) to block spammers' mail without the threat of being sued by the spammers. For more information on CAN SPAM, click here.

Hold the Pickle! Hackers Cause Trouble at Burger King

Some customers ordering from the drive thru window at a Burger King in Troy, Michigan, received a shock when the responses from the other end weren't what they expected. Some teenagers apparently hacked into BK's wireless frequency and were responding to customers with such quips as, "You don't need a couple of Whoppers. You're too fat! Pull ahead." For more info on this story, check out the article available at Ananova.com.

Trojan Masquerading as XP Service Pack

January 9, 2004. A Trojan horse known as *Xombe* or *Downloader GJ* has been reported to be masquerading as a Microsoft Windows XP service pack. The malicious code is being distributed widely and appears to be a legitimate email from windowsupdate@microsoft.com; however, the address has been spoofed. The email contains a subject line that reads "Windows XP Service Pack 1 (Express) - Critical Update" and contains the attachment, winxp_sp1.exe. If the attachment is run, it attempts to download another .exe which then launches a denial of service attack against a Russian website. If you do receive an email like the one described above, do not open the attachment. Notify your network administrator immediately. He/she will advise you on the appropriate action to take. For more information on this threat, click here. Information on Kentucky State Government's malicious code policy and procedures can be found in the Commonwealth's Enterprise Anti-Virus Policy (CIO-073).

Microsoft Updates

Microsoft has released the following security updates this month for its operating systems and other software products. GOT recommends that agencies devise procedures to ensure the timely installation of hardware and software patches/updates, as well as the update of virus definition files. A comprehensive list of hardware and software security vulnerabilities can be found on the GOT Security Alert webpage.

Microsoft Security Bulletin MS04-001

Vulnerability in Microsoft Internet Security & Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution (816458)

A security vulnerability exists that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000.

Microsoft Security Bulletin MS04-002

Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (832759)

Exchange Server contains a vulnerability that could allow an authenticated user to connect to another user's Outlook Web Access (OWA) mailbox.

Microsoft Security Bulletin MS04-003

Buffer Overrun in MDAC Function Could Allow Code Execution (832483)

Microsoft has reported a buffer overrun in a MDAC function that code when handling broadcast response data that may allow code execution.

Upcoming Microsoft Webcast Offerings

TechNet Webcast: Designing a Secure - Reliable - and Usable Patch Management Infrastructure
1/21/2004-11:30 AM - 1:00 PM Pacific Time, US & Canada

MSDN Webcast: Best ASP.NET Practices for Shielding Your Site from Hackers
1/22/2004 - 1:00 PM - 2:30 PM PST

TechNet Webcast: Implementing Security Patch Management
1/27/2004-9:30 AM -11:00 AM Pacific Time, US & Canada

TechNet Webcast: Software and Patch Management with Software Update Service, Windows Update and SMS
1/28/2004-11:30 AM - 1:00 PM Pacific Time, US & Canada

TechNet Webcast: Implementing Client Security on Windows 2000 and Windows XP
1/28/2004-8:00 AM - 9:30 AM Pacific Time, US & Canada

MSDN Webcast: ASP.NET Security Best Practices
1/28/2004-9:00AM-10:30AM Pacific Time, US & Canada

If you can't attend the live webcasts, check out the many on-demand webcasts available here.

KENTUCKY GOVERNOR'S OFFICE FOR TECHNOLOGY

Division of Security Services
101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502-564-7680

Email:
GOTSecurityServices@ky.gov

We're on the Web!
ky.gov/got/security/

The information contained in this newsletter is intended for internal use only.

GOT's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security & information systems professionals with timely information on cyber vulnerabilities, information security trends, virus info, and security policies & practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of the GOT Security Policies and Procedures Manual (SPPM), GOT's disaster recovery/ business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, and Unix Solaris & AIX systems. DSS also provides mainframe RACF, computer forensics, and password auditing services to state agencies upon request. If you would like to learn more about the services that DSS provides, visit our web page.

For more information on IT Security, check out the following websites!

www.cerias.purdue.edu—The Center for Education and Research in Information Assurance and Security (CERIAS) is currently viewed as one of the world's leading centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure.

www.itsecurity.com—The encyclopedia of computer security. ITSecurity.com is a free site for anyone interesting in IT security. The site has over 10,000 pages on security that are updated frequently.

www.infosyssec.org—The most comprehensive computer and network security resource on the Internet for information system security professionals.

www.whitehouse.gov/pcibp—Government website that contains the national US strategy to secure cyberspace.

www.staysafeonline.info—Site sponsored by the National Cyber Security Alliance. Provides information on security your personal computer.

isc.incidents.org—Global Internet Storm Center. Tracks and monitors Internet activity and threats. This sites compiles current global Internet activity data to provide visitors current status of the Internet.

Microsoft's IT Pro Security Zone—Microsoft bulletin board with the latest info on Microsoft patches, virus threats, and other security-related information.